Analysis of the Congruence Expression for testing if n is prime.

$$2^{n-1} - 1 \equiv 2^n - 2 \pmod{n}$$

Mar Detic

Abstract

This paper analyzes the congruence expression $2^{n-1} - 1 \equiv 2^n - 2 \pmod{n}$, exploring its validity for different values of n. We test the expression for both prime and composite numbers, and observe that the congruence holds for primes but does not hold in general for composite numbers.

1 Introduction

We are interested in testing the congruence expression:

$$2^{n-1} - 1 \equiv 2^n - 2 \pmod{n}.$$

This expression involves powers of 2 modulo n and is worth exploring due to its potential applications in number theory. In this paper, we investigate whether this congruence holds for both prime and composite values of n.

2 Mathematical Analysis

We begin by simplifying both sides of the given expression.

2.1 Left-Hand Side (LHS)

The left-hand side of the expression is:

$$2^{n-1} - 1.$$

This is a simple expression involving the power of 2 reduced by 1.

2.2 Right-Hand Side (RHS)

The right-hand side of the expression is:

$$2^n - 2.$$

We can rewrite this as:

$$2^n - 2 = 2^{n-1} \cdot 2 - 2.$$

Thus, the congruence we are testing is:

$$2^{n-1} - 1 \equiv 2^{n-1} \cdot 2 - 2 \pmod{n}.$$

This simplifies to checking whether the following holds true:

$$2^{n-1} - 1 \equiv 2^{n-1} \cdot 2 - 2 \pmod{n}.$$

3 Empirical Testing

We now test this congruence for different values of n, including both prime and composite numbers.

3.1 Test Case: $n = 5$

For $n = 5$, we compute the left-hand side (LHS) and right-hand side (RHS):

$$\text{LHS} = 2^{5-1} - 1 = 2^4 - 1 = 16 - 1 = 15.$$
$$\text{RHS} = 2^5 - 2 = 32 - 2 = 30.$$

Now, check modulo 5:

$$\text{LHS modulo } 5 = 15 \mod 5 = 0,$$
$$\text{RHS modulo } 5 = 30 \mod 5 = 0.$$

Thus, for $n = 5$, the congruence holds: $\text{LHS} \equiv \text{RHS} \pmod{5}$.

3.2 Test Case: $n = 7$

For $n = 7$, we compute the left-hand side (LHS) and right-hand side (RHS):

$$\text{LHS} = 2^{7-1} - 1 = 2^6 - 1 = 64 - 1 = 63,$$
$$\text{RHS} = 2^7 - 2 = 128 - 2 = 126.$$

Now, check modulo 7:

$$\text{LHS modulo } 7 = 63 \mod 7 = 0,$$

$$\text{RHS modulo } 7 = 126 \mod 7 = 0.$$

Thus, for $n = 7$, the congruence holds: $\text{LHS} \equiv \text{RHS} \pmod 7$.

3.3 Test Case: $n = 9$

For $n = 9$, we compute the left-hand side (LHS) and right-hand side (RHS):

$$\text{LHS} = 2^{9-1} - 1 = 2^8 - 1 = 256 - 1 = 255,$$
$$\text{RHS} = 2^9 - 2 = 512 - 2 = 510.$$

Now, check modulo 9:

$$\text{LHS modulo } 9 = 255 \mod 9 = 3,$$

$$\text{RHS modulo } 9 = 510 \mod 9 = 6.$$

Thus, for $n = 9$, the congruence does not hold: $\text{LHS} \not\equiv \text{RHS} \pmod 9$.

4 Conclusion

Based on the empirical testing for $n = 5$, $n = 7$, and $n = 9$, we observe the following:

- For prime numbers $n = 5$ and $n = 7$, the congruence holds.
- For composite numbers $n = 9$, the congruence does not hold.

Therefore, it appears that the congruence $2^{n-1} - 1 \equiv 2^n - 2 \pmod n$ holds true for prime values of n, but not for composite numbers in general.